UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-v- Criminal No. 5:16-CR-0096 (MAD)

MACKENZIE STACEY,

Defendant.

MEMORANDUM OF LAW IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE DERIVED FROM AN UNLAWFUL SEARCH AND SEIZURE AND FOR A HEARING PURSUANT TO *FRANKS V. DELAWARE*

DATED: FEBRUARY 17, 2017
Albany, New York

Respectfully submitted,

LISA A. PEEBLES
Federal Public Defender

By: PAUL J. EVANGELISTA, Esq.
First Assistant Federal Public Defender
Bar Roll No.: 507507
MOLLY CORBETT, Esq on Brief
OFFICE OF THE FEDERAL PUBLIC DEFENDER
39 North Pearl St., 5th Floor
Albany NY 12207
(518) 436-1850

Table of Contents

I. INTRODUCTION

The defendant, MACKENZIE STACEY, moves this Court pursuant to Fed. R. Crim. P. 12(b)(3)(c) for an order suppressing all evidence seized from his computer, media storage devices and private on-line accounts, by the FBI or other law enforcement authorities beginning January 16, 2015 to October 30, 2015. The evidence seized was the result of unconstitutional government acts which included the Government's deployment of malware referred to as a "Network Investigative Technique," (NIT) which was inserted by FBI agents in Virginia onto Mr. Stacey's computer in Earlton, New York. The application of a search warrant for Stacey's Earlton, New York residence and the execution of the warrant at the Earlton, New York residence.

The government's insertion of the NIT virus affirmatively altered and overrode security and privacy settings on the defendant's computer allowing the FBI to remotely access, search, and seize data on the computer's hard drive without a proper warrant. That information was then seized and removed from the computer and transmitted to FBI agents in Virginia. Mr. Stacey seeks suppression of all fruits of this illegal search on eight grounds:

First, the remote search of Mr. Stacey's home computer was undertaken pursuant to a warrant that was not supported by probable cause. As set forth below, the Government sought and received authorization to search the computers of anyone who visited the homepage of a website called "Playpen." *See* Ex. 1 (the NIT warrant and supporting application). The resulting warrant was effectively a general warrant, which authorized an unlimited number of searches anywhere in world. The NIT warrant ultimately authorized over 100,000 searches around the world. As a result, the absolute scope of the searches and resulting seizure by the Government of

information in this case and others is unprecedented in our history, and legitimizing this tactic would set a disturbing precedent for the future of our privacy.

Second, the FBI intentionally or recklessly misled the issuing court about how the site appeared, among other false and misleading statements. Specifically, the warrant application alleged that the site's home page displayed purportedly lascivious pictures that advertised illegal content on the site. Upon information and belief, the content of the site's home page arguably was not lascivious and a hearing is necessary to determine whether the representation of the content was misrepresented or other information omitted influencing the issuing judge's determination. Questions have also arisen as to the actual content of the site at the time of the application for the warrant. The FBI had seized control of the site before applying for the warrant and now claims no knowledge of the change in content. The defense therefore requests a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978) to determine whether the officers knew at the time of the execution of the warrant that the warrant had misrepresented the content and whether other omissions affected the probable cause determination. Probable cause for these searches turns on whether the website "unabashedly announced" that it was dedicated to illicit child pornography. Playpen (also known as "Website A") had a mix of legal and illegal content including chat and messaging forums and did not advertise itself as a child pornography website.

Third, the NIT warrant is unconstitutionally overbroad and is essentially a general warrant. The warrant authorized searches anytime an individual accessed the Playpen homepage rather than when they accessed or attempted to access child pornography located in sub-directories. Because the FBI was operating the website, it would have been easy to narrow the warrant to those who viewed or downloaded child pornography.

Fourth, the NIT warrant was an anticipatory warrant with a premature "triggering event"

that authorized a search before probable cause was established. As set forth in the warrant application, the triggering event was the act of visiting Playpen's home page as it was described in the warrant application and then merely clicking to enter the site. However, the triggering event did not occur in this case because the FBI had included a false description of the home page in the application. The home page as it actually appeared at the time the warrant was issued and the searches were executed did not, as the FBI had claimed, suggest that the site contained child pornography. The search in this case therefore exceeded the scope of the warrant's authorization and suppression is required.

Fifth, the NIT warrant was issued in the Eastern District of Virginia (E.D.V.A.) and it only authorized searches of persons or property located in that district. Consequently, the search of Mr. Stacey's New York computer exceeded the scope of the Eastern District of Virginia warrant.

Sixth, if the NIT warrant purportedly authorized searches outside the district in which it was issued then the warrant violated Fed. R. Crim. P. 41. This violation was of a constitutional magnitude and requires the suppression of evidence that is seized in violation of Rule 41's jurisdictional limitations.

Seventh, the later search warrant for 3461 Schoharie Turnpike, Earlton, New York dated October 29, 2015 and executed the next day, was based upon fruits of an illegal search and as such was invalid. (Ex. 3, Earlton Search Warrant).

Eighth, the statements made by Mackenzie Stacey on October 30, 2015 are subject to suppression as they were made in violation of *Miranda v. Arizona* and the Fifth Amendment due process clause. Any information derived from those statements is also subject to suppression as "fruit of the poisonous tree".

II. STATEMENT OF FACTS

On October 30, 2015, FBI agents executed a search warrant at the home of the defendant, Mackenzie Stacey, in Earlton, New York, and seized (among other items) two personal computers. Mr. Stacey was home at the time of the search as was his father Richard Stacey, Lydia McCormick, and his sister, Maegen Stacey. This search was the second search of Mr. Stacey's property, the first having occurred in February 2015, when the FBI used a "Network Investigative Technique" (NIT) to insert malicious code onto his computer to search for and seize data stored on the computer. This initial search and seizure from February to March of 2015, and the action of law enforcement on October 30, 2015 are the focus of Stacey's request to suppress based upon constitutional violations, failing to comply with applicable statutory requirements and criminal procedures.

The events leading to the search of Mr. Stacey's home, the seizure of property from within the home and his statements to law enforcement began in December 2014, when a "foreign law enforcement agency" happened upon the website "Playpen", learned that it contained child pornography, and alerted the FBI. See *United States v. Levin*, 2016 WL 2596010, *1 (D. Mass. 2016)(*Westlaw only*); Ex. 1, ¶28 (the NIT warrant application). Playpen operated on a network commonly known as the "Tor" network. *Id.* Tor was created by the U.S. Naval Research Laboratory and it is primarily funded by the U.S. Government. The network is designed to "protect user privacy online." Ex. 1at ¶¶ 7-9. In simple terms, anyone who wants to use the Tor network can download a free browser and search engine (similar to Chrome or other Internet browsers) that provides added privacy protections. *See* https://www.torproject.org ("Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities

and relationships, and state security."). Activities and communications on Tor (like visiting a website) are routed through multiple computers (or "nodes") to protect the confidentiality of the Internet Protocol (IP) addresses and other identifying information of its users. Ex. 1 at ¶¶ 7-9.

Like the Internet in general, the Tor network can be used for both legitimate and illicit purposes. *See* Virginia Hefferman, *Granting Anonymity*, N.Y. Times, December 17, 2010 ("Peaceniks and human rights groups use Tor, as do journalists, private citizens and the military, and the heterogeneity and far flungness of its users – together with its elegant source code –keep it unbreachable."). Millions of people now routinely use the Tor network to avoid being targeted by advertising, to protect their personal data from marketing companies and scammers, and to search for a wide variety of content that they wish to keep private.

Due to an error in Playpen's connections with the Tor network, it could be found and viewed on both the Tor network and the regular Internet for at least part of the time that it was operating. The FBI was able to locate the operator of Playpen and raided his home in Naples, Florida, in February 2015. Ex. 2 (Application for an Order Authorizing Interception of Electronic Communications dated February 20, 2015.), ¶38.

A. The FBI's Distribution of Pornography from Playpen

After raiding the operator's home, the FBI did not shut Playpen down. Instead, the FBI took control of Playpen and moved its server to a government facility in Virginia where it maintained and operated the site at least until March 4, 2015. Ex. 2, ¶38. During this time the FBI continued to operate the site as an active distributor of child pornography and took no measures to block or limit the uploading, downloading or redistribution of thousands of illicit pictures and videos. Upon information and belief, the FBI upgraded the website to improve ease

of access and storage capacity.[1] When the FBI took over Playpen on February 20, 2015, the site had 158,094 members. Ex. 2 at ¶ 18.

B. The Virginia "Network Investigative Technique" Warrant ("NIT Warrant")

On February 20, 2015, the Government submitted its application for the use and deployment of a "Network Investigative Technique" or NIT. The NIT warrant application was submitted to Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia. In the application, Playpen was described as a "child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children." Ex. 1, Macfarlane Affidavit, p.5, ¶ 6. More accurately, Playpen offered a mix of chat forums, private messaging services, both legal and illegal pictures and videos, and links to pictures and videos. *See* Ex.1. Macfarlane Aff. p. 15, ¶ 14.

The warrant application sought authorization to use a "Network Investigative Technique" to search "activating computers," defined as the computers "of any user or administrator who logs into the TARGET WEBSITE by entering a username or password." Ex. 1, "Attachment A". The username and password could be made up and entered on the spot (there was no verification or other steps required to enter the site), and the site was free. Somewhat confusingly, the actual targets of the NIT warrant and search were the "activating computers," not the "TARGET WEBSITE," referring to Playpen. Not only had the FBI already seized Playpen, its server and records which did not contain any of the visitor data the FBI wanted to search for pursuant to the

[1] Based upon information provided from other federal public defenders from the analysis of discovery in other Playpen cases. The parties are working through discovery and the government has been very receptive to defense requests. The defense expects the same information provided in other cases around the country will be provided. If said information is not forthcoming, counsel will move to compel production, seek additional input from an expert associated with these cases and/or move to unseal the materials in other Playpen cases to obtain the information.

warrant. Ex. 1, Macfarlane Aff. pp. 21-22, ¶¶28-30. Nor could that data be collected from third parties, such as Time Warner or other Internet service providers, since the basic purpose of the Tor browser and network is to privatize its users' identities and activities. Ex. 1, Macfarlane Aff. pp. 10-13, ¶¶ 7-11.

Accordingly, the warrant application explained that the FBI would use its NIT to search for data directly on the personal computers and other digital devices of anyone who visited the Playpen site. This data included user addresses; the type of operating systems on their computers; and various other private data that would not otherwise be disclosed by a computer's owner or user. *Id.* at 25, ¶ 34. Elsewhere in the application, the NIT was broadly described as hidden "computer instructions," or code, that agents would send to the unidentified, non-specific targets when they landed on the home page and typed in a name or password. *Id.*[2]

Once the FBI had inserted a NIT onto an activating computer, it would do several things to execute a search on and seize data from that computer. First, the NIT altered or overrode a computer's security settings to install itself on the targeted computer, similar to disabling a home's burglar alarm system before climbing through a window. Next, the NIT searched the computer's hard drive and operating system for the data that the FBI wanted. Ex. 1, Attachment B (listing specific information to be obtained). This examination is technically equivalent to searching locked desks or file cabinets in a house to find an address book, billing records or maps containing some information the FBI was looking for and that information then telling them where and how to find more information. Finally, the NIT overrode the user's Tor browser protections and forced the computer to send the seized data back to the FBI, where it was stored

[2] The agent applying for the warrant attempted to assure the issuing court of their intent to limit its application stating that although the request allowed for the deployment of the NIT to "any user who logs into the TARGET WEBSITE" the FBI intended to deploy the NIT more discreetly to ensure technical feasibility and avoid detection. Ex. 1, ¶32. n. 8

in the digital equivalent of an evidence room on a government server.

Playpen had a mix of legal and illegal content, as well as chat forums, and the NIT warrant application did not allege that everyone who visited the site necessarily viewed illegal pictures, nor did it confine the use of the NIT to only those users who were accessing or providing alleged illegal content. In fact, the FBI had assured the judge that "in executing the requested warrant, the FBI may deploy the NIT more discretely" against those who had attained a higher status on the website by substantial posting activities in particular areas of the site or sub-forums. Ex. 1, Macfarlane Aff. pp. 24-25, ¶33, n. 8.

Upon information and belief, the homepage of the website did not suggest that it contained child pornography.[3] The warrant application nevertheless sought authorization to search the computers of anyone who simply passed through the home page. The affiant focused on the appearance and contents of the home page in an attempt to establish probable cause to believe that anyone accessing the site was committing a crime. The application describes the home page as containing a banner with "two images depicting partially clothed prepubescent girls with their legs spread apart." Ex. 1, Macfarlane Aff. pp. 13-14, ¶ 12. The application did not claim that these pictures met the legal definition of "lascivious" pornography, in 18 U.S.C. § 2256(2)(A), and the application did not include a copy of the home page.

Moreover, this description of the homepage in the NIT warrant application is inaccurate. From discovery from *United States v. Michaud* 3:15-CR-5351 and pre-trial submissions in other Playpen cases, the defense has learned that a screen shot had been taken on February 3, 2015 (17 days prior to the warrant application). *Infra.* Note 1. The home page, as it actually appeared from

[3] Counsel has requested a copy of the home page as it existed at the time of the warrant applications but has not yet received a copy of the screen shot. The contents of two versions of the home page are known from other prosecutions involving this website and discussion with other assistant federal public defenders.

February 19, 2015 (the day before the warrant application) until the site was shut down, was devoid of any sexualized images of prepubescent girls as was alleged in the EDVA affidavit, and instead merely showed a picture of a fully clothed female who could be a young adult with her legs crossed. While the woman depicted on the home page appears to be young, the image is small and it is not at all clear that she is under the age of 18, let alone "prepubescent," nor does the pose appear lascivious. In addition, there is a question as to whether the other version of the landing page would be represent that the site contained child pornography based upon the image on the landing page at the time of the application for the warrants.

The rest of the material in the NIT warrant application about the site describes child pornography that could be found in various sub-directories. After signing in to Playpen, visitors were directed to a "table of contents" listing 46 different forums and sub-directories. Ex. 1, Mcfarlane Aff., pp. 15-17, ¶ 14 (listing contents of website); Ex. 2, Bletsis Affidavit, pp. 16-17, ¶21 Like the home page, the table of contents did not contain child pornography (the graphics on the page depict onions, a visual reference to the Tor network) and it listed a variety of topics. Id. Most of these relate to sexual matters or fetishes, and some of these also relate to children. Id.

However, the table of contents could be viewed only *after* someone had logged into the site, at which point the FBI had already deployed and remotely searched the visitor's computer. Ex. 1, McFarlane Aff., pp. 15, ¶14; Ex. 2, Bletsis Aff., p. 16, ¶21. From there, in order to locate pictures or videos, a visitor would have to take the additional steps of selecting one of the sub-directories with a suggestive title; clicking on or opening the sub-directory; and then scrolling through its content to view what was actually displayed. Intentionally downloading or copying any of the pictures or videos on view would require additional steps. Clicking on one of the links

which clearly advertised child pornography would have been a more appropriate triggering event for deployment and use of the NIT, rather than searching everyone who simply landed on and entered the homepage.

C. The Authorized Search Locations

The cover sheet of the NIT application identifies the locations to be searched pursuant to the warrant in a sworn statement that reads as follows:

> I, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property. . . *located in the Eastern District of Virginia*, there is now concealed . . . (see attachment B).

Ex. 1.

Consistent with this statement, the warrant itself specifies the location to be searched as "property located in the Eastern District of Virginia." Ex. 1. Search and Seizure Warrant dated February 20, 2015. The warrant then refers to "Attachment A" to more particularly describe the "property to be searched" within that district. Attachment A first lists the "TARGET WEBSITE," "which will be located at a government facility in the Eastern District of Virginia." Id. As noted, "Target Website" refers to the Playpen server that had already been seized, and none of the data sought by the FBI was stored on or available from that server. "Attachment A" then lists "activating computers" as additional places to be searched, and describes them as "those of any user or administrator who logs into the TARGET WEBSITE." The attachment fails to identify any locations other than EDVA, nor does it state that "activating computers" may be located outside the district or otherwise modify the affiant's averment on the application's first page that searches would extend only to targets within the district.

D. The Warrant and Application for the Search of 3461 Schoharie Turnpike, Earlton, New York ("Earlton Warrant").

According to the warrant application submitted to Magistrate Judge Hummel in the Northern District of New York by Special Agent Benjamin Paris, probable cause existed for the search of 3461 Schoharie Turnpike, Earlton, New York because a Mid-Hudson Cablevision internet account registered to Lydia McCormick at the SUBJECT PREMISES and assigned IP address 24.105. 215.177 was linked to an online website referred to as "Website A." Paris alleged that Website A was used to regularly send and receive child pornography on an anonymous online network. Ex. 3, Paris Affidavit, p. 13, ¶13. The IP address assigned to this Mid-Hudson internet account for the relevant period of February 2015 through March 2015 had been linked through IP logging information obtained by law enforcement officers to Website A. The application alleged there was probable cause to believe that an individual using the internet account at the SUBJECT PREMISES received, distributed and accessed with intent to view child pornography on Website A. Ex. 3, Paris Aff. p.10, ¶7.

The Probable Cause section also explained how "the Network" was set-up and functioned. Ex. 3, Paris Aff., pp. 11-12, ¶¶8-12. Agent Paris did not provide the name, but from other filings, it is now known to be a reference to the Tor network. The Probable Cause section also included a "Description of Website A and its Content." Ex. 3, Paris Aff. pp. 13-17, ¶¶13-23. None of the information in this section was specific to the use of any computer at the Earlton, NY residence or an IP address related to the address to be searched. Instead it was a summary of the content of sub-forums which was arguably obtained by an agent other than Paris since the FBI ceased operating the website in March of 2015.

Special Agent Paris advised that the FBI began searching computers using the NIT on February 20, 2015, the same day the NIT warrant was granted by Judge Buchanan. Data from the logs of Website A showed a user, identified as "Shitbucket" opened an account on January 16,

2015 as a "Newbie member," lacking a senior designation. Ex. 3, Paris Aff., p. 19, ¶ 27. The affidavit also stated that data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, on February 28, 2015 at 22:10 UTC showed the user "Shitbucket" logged into "Website A" from IP address 24.105.215.177 using a username and password combination. The account accessed a post entitled "Camille (Violet) 9 HD videos + 51 Thumbnails - ALL THAT I HAVE" which contained at least one image of child pornography. Ex. 3, Paris Aff., p. 19. ¶28. The user also browsed "Website A" after logging in with a username and password when the user's IP address information was not collected. The user's account allegedly accessed two images of child pornography, on February 21, 2015 and on March 01, 2015. Ex. 3, Paris Aff., pp. 19-20, ¶29.

Using information from public websites FBI Special Agents were able to determine that IP address 24.105.215.177 was operated by an ISP called Mid-Hudson Cablevision. Ex. 3, Paris Aff., p. 20, ¶30. A response to an administrative subpoena/summons served on Mid-Hudson Cablevision requesting information related to the account assigned IP address 24.105:215.177 indicated that, the IP address was assigned to an account in the name of Lydia McCormick at 3461 Schoharie Turnpike, Earlton, New York and was current as of June 05, 2015. Ex. 3, ¶30. Further surveillance and research of the address revealed that Lydia McCormick, Richard Stacey, Mackenzie M. Stacey and Maegen G. Stacey resided at the address as of June 2015. Ex. 3. Paris Aff., pp. 20-21, ¶¶31-32.

The warrant application for 3461 Schoharie Turnpike, stated that the NIT caused the user's computer to send:

> a. the computer's actual IP address and the date and time that the NIT determined what that IP address was;
> b. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers;
> c. details of the operating system running on the computer, including type (e.g.,

Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
d. information about whether the NIT had already been delivered to the computer;
e. the computer's Host Name;
f. the computer's active operating system username; and
g. the computer's media access control ("MAC") address.

Ex. 3, Paris Aff., pp. 18-19, ¶26.

Sometime after February 20, 2015, presumably sometime on February 21, 2015, FBI agents sent the NIT virus to a computer connected to someone with the username "Shitbucket" and then seized the listed data from the computer presumably associated with the IP address.

Upon information and belief, the FBI used the data and other information it had seized from the computer in the Earlton, New York residence, to prepare an administrative subpoena to Mid-Hudson Cablevision to obtain account holder identity and physical address information. Mid-Hudson responded with Ms. McCormick's subscriber information, name and address and the FBI added that information to the data it had acquired through the use of the NIT.

On October 29, 2015, the Hon. Christian Hummel issued a warrant authorizing the search of the residence and any computers located therein. Ex. 3. On October 30, 2015, eleven FBI and other law enforcement agents executed the search warrant at 7:30 a.m. on the three bedroom mobile home. Exhibit 4. Ms. McCormick, Richard Stacey, Maegen Stacey and Mackenzie Stacey were present. Ex. 4. The agents searched the home. During the search certain agents performed preliminary searches of the computers within the home, Exhibit 5. Two hard drives and two media storage devices were eventually seized.

SA Paris initially spoke with Mr. Stacey's father, Richard Stacey and Linda McCormick. During that conversation, Paris was told who lived at the home. Ex. 5. Further discussions with Richard Stacey resulted in the elder Stacey being informed of the nature of the investigation and also being advised of his *Miranda* rights. Exhibit. 6. Stacey executed a consent to questioning

and admitted using the Tor network, and viewing legal pornography but denied viewing or downloading child pornography. Ex. 5.

SA Paris and SA Fallon then moved on to questioning the defendant, Mackenzie Stacey. Ex. 5.[4] Mackenzie identified his computers within the home and denied viewing child pornography. Id. He advised that he viewed legal pornography which he views and deletes. Id. He also spent significant amounts of time playing games on-line. Id. He stated he had used the Tor network in the past but stopped because he did not need the anonymity Id. SA Paris took a break from questioning Mackenzie and learned that an examination of a computer had the same MAC address and computer name as one accessing Website A. Id. SA Paris and Fallon then advised Mackenzie of his *Miranda* rights which he waived. Ex. 6. Mackenzie then admitted to accessing Website A, viewing and deleting child pornography. Id. An Assistant United States Attorney was contacted. Mackenzie was placed in handcuffs and taken to FBI headquarters in Albany. He was arraigned before the magistrate judge at 2:00p.m. and released on conditions. Ex. 5.

At all times during the execution of the search warrant and questioning of both Richard Stacey and Mackenzie Stacy law enforcement agents remained in and around the home. (Exhibit 8, Declaration of Mackenzie Stacey). During the questioning of Mackenzie, he was continually in the company of SA Paris and SA Fallon or SA Fallon. At no time was Mackenzie free to leave.

Mackenzie Stacey has been indicted. The defendant is charged by indictment with one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B); and two counts of receiving child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A).

[4] The statements attributed to Mackenzie Stacey are taken from the accounts of the agents and are in no way adopted by Mr. Stacey as an accurate representation of his statements. He reserves his right to challenge that accuracy.

III. ARGUMENT

A. The NIT Warrant Was Not Supported by Probable Cause

The affidavit supporting the NIT warrant did not establish probable cause for the original search of Mr. Stacey's computer. The NIT warrant authorized the FBI to search the computers of any and all visitors to Playpen from the moment they entered a name and clicked 'Log In' on the home page. *See* Ex. 1, Macfarlane Affidavit, p. 24, ¶ 32. The warrant sought sweeping authority "to investigate any user or administrator *who logs into* the TARGET WEBSITE by entering a user name and password" (emphasis added). *Id*. The user name and password could be made up and entered on the spot, and the site did not charge any fees. Nor did it verify user information or otherwise require affirmative steps to access the site. The website's homepage did not suggest that it contained child pornography; it simply had a banner that read "PlayPen" and a picture of clothed females.

The Second Circuit has held that an affidavit which merely alleges a suspect "appeared either to have gained or attempted to gain access" to a child pornography website—without more—does not constitute probable cause sufficient to issue a search warrant. *United States v. Falso*, 544 F.3d 110, 120 (2d Cir. 2008). Thus, "the mere fact the defendant had apparently tried to access a non-membership website featuring images of child pornography, absent any evidence that he subsequently viewed those images, [does] not establish probable cause to search his computer." *United States v. Raymonda*, 780 F.3d 105, 116 (2d Cir. 2015). The Second Circuit has had several occasions to consider the sufficiency of affidavits filed in support of search warrants based on information obtained from an FBI investigation into child pornography websites. *See Falso*, 544 F.3d 110, 120 (2d Cir. 2008); *United States v. Martin*, 426 F.3d 68, 71 (2d Cir. 2005); *United States v. Coreas*, 419 F.3d 151, 151 (2d Cir. 2005). In so doing, the

Circuit articulated factors necessary to find that sufficient probable cause exists in a residential warrant related to suspected access of child pornography websites. *Martin*, 426 F.3d 68, 71 (2d Cir. 2005). The factors include

> (1) Whether the e-group's welcome page and title . . . made plain its essential purpose to trade child pornography of minors;
> (2) the affidavit's discussion of the modus operandi of those who use computers to collect and distribute child pornography;
> (3) the affidavit's description of the characteristics and proclivities of child-pornography collectors, including their tendency to collect pornographic images;
> (4) the fact that the e-group's illicit purpose could be inferred from the website's technological features that facilitated trading in child pornography;
> (5) the affiant's confirmation that the e-group contained child pornography available to all members;
> (6) the fact that the defendant lived at the house to be searched; and
> (7) the fact that the defendant was an e-group member who joined voluntarily and never cancelled his membership. *Id*. at 75-76

The most critical factors articulated as support for probable cause by the Second Circuit are conspicuously absent in the present case. Here, the website's welcome page and title did not make plain that its essential purpose was related to child pornography. Therefore, probable cause for the computer searches turned on the contents of the home (or "log in") page and whether it was likely that anyone who saw that page would know that its contents were illegal before proceeding to actually take a look at the contents. *United States v. Martin*, 426 F.3d 68, 71 (2d Cir. 2005). Secondly, the technological features of the website did not create an inference that it facilitated trading child pornography. A log-in associated with an email and username with instructions about privacy is not solely indicative a child pornography web site. Thirdly, the affidavit requested a warrant to search anyone who merely logged into the website, completely disregarding whether they were aware it contained child pornography when they first accessed

it.[5] While the warrant application asserted that Playpen "advertised" that it was "dedicated" to child pornography, even the most cursory review of its home page shows that this is not correct.

The only fact that would suggest the site may have contained child pornography is the description of pictures that appear on the site's banner, "located to either side of the site name," "depicting partially clothed prepubescent females with their legs spread apart." Ex. 1. The affiant did not claim that these pictures met the definition of illegal "lascivious" images, and in fact they do not. *See generally United States v. Rivera*, 546 F.3d 245, 250-53 (2d Cir. 2008); *United States v. Battershell*, 457 F.3d 1048, 1051 (9th Cir. 2006) (photograph described as "a young female (8–10 YOA) naked in a bathtub" is "insufficient to establish probable cause that the photograph lasciviously exhibited the genitals or pubic area"); *United States v. Brunette*, 256 F.3d 14, 17 (1st Cir. 2001) (statement that images showed "'a prepubescent boy lasciviously displaying his genitals'" was a "bare legal assertion, absent any descriptive support and without an independent review of the images, [which] was insufficient to sustain . . . probable cause"). Nor did either affiant include a copy of the home page with the warrant application so that Magistrate Judge Buchanan could assess it for herself

As a result, the affidavit – even if it had been accurate – did not establish probable cause to install malicious code which searched and removed data from the computers of everyone who stumbled upon the website and simply entered a user name and password on the spot. Without any pictures that are even arguably "lascivious," there is nothing to suggest that Playpen advertised or promoted itself as a child pornography site. Given the facts alleged in the affidavit, there can be no reasonable dispute that the critical information for probable cause purposes was

[5] Even the Government appeared concerned with the breadth of the search's potential which was created by requesting a search based solely upon a log-in and a user name. In his affidavit McFarlane assured the court that the searches would be constrained to the users of the website who were the more veteran users with demonstrated histories of posting and contributing to the site. Ex. 1, p. 24, ¶32, n. 8.

the claim that the site displayed "partially clothed prepubescent females with their legs spread apart" and the suggestion, at least, that these images were "lascivious" and illegal.

The law is clear that when a computer search is based on someone's mere accessing of a website, there is probable cause for a search only if the site's illegal purpose or content is readily apparent. *Falso*, 544 F.3d 110, 120 (2d Cir. 2008). The Second Circuit adopted the Ninth Circuit's approach in *Gourde* that there is probable cause for a search only if the site's illegal purpose or content is readily apparent. *Falso*, 544 F.3d 110, 120 (2d Cir. 2008) citing *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006). Unlike here, the site in *Gourde* was quite explicit about what it offered. First, the name of the site in *Gourde* was "Lolitagurls.com," and the term "Lolita" is commonly and exclusively associated with a prurient focus on young girls. *Id.* at 1014; *see also United States v. Shields*, 458 F.3d 269, 279 (3d Cir. 2006) (explaining the use of the term "Lotita" and connection with child pornography).

Here, by contrast, the affiant did not allege that the site's name had any connection to child pornography. Further, unlike Playpen's home page, the *Gourde* home page explicitly advertised the number and quality of its "Lolita pics," noting the amount, their status as unclothed minors, "[o]ver one thousand pictures of girls age 12-17! Naked lolita girls with weekly updates! What you will find here at Lolitagurls.com is a complete collection of young girl pics." 440 F.3d at 1067. In stark contrast to Playpen, the site in *Gourde*, like that in *United States v. Martin*, 426 F.3d 68, 75 (2d Cir. 2005), "unabashedly announced that its essential purpose was to trade child pornography." *See also, e.g., Shields*, 458 F.3d at 278 (agreeing with *Martin*'s characterization of a site as one that ""unabashedly announced that its essential purpose was to trade child pornography").

Significantly, the site in *Gourde* implicated even more of the Second Circuit's *Martin*

factors because the website there charged a membership fee and visitors saw "images of nude and partially-dressed girls, some prepubescent" *before* they paid the fee and joined the site. Unlike Playpen, which was free and immediately accessible, the court found that the defendant in *Gourde* had demonstrated his intent to view and download child pornography because, *after* having viewed samples of the illicit pictures offered on the site, he took the additional "affirmative steps" of entering his credit card information, paying a monthly fee, and maintaining his membership for at least two months. *Gourde*, 440 F.3d at 1071 ("The affidavit left little doubt that Gourde had paid to obtain unlimited access to images of child pornography knowingly and willingly, and not involuntary[il]y, unwittingly, or even passively"). Here the application does little more than allege probable cause based upon logging in and accessing the site without specificity to the acts of each defendant or persons subsequently monitored because of that access.

Although the Second Circuit in *Martin* upheld the sufficiency of an affidavit filed in support of a search warrant of a defendant's residence based on information obtained from an FBI investigation into child pornography e-groups, the majority affirmance was supported by a laundry list of facts not present in the case against Stacey. See *Martin*, 426 F.3d at 75-77 (listing the numerous facts supporting probable cause with the first being the e-group's welcome page and title, "girls 12-16," which made plain "its essential purpose to trade child pornography" of minor girls). The majority deemed it "common sense" that "an individual who joins such a site would more than likely download and possess such material," and concluded that the affidavit, as corrected to eliminate statements determined to be false, established probable cause for the search warrant.

Given these facts, the court found that the warrant application in *Martin* and *Gourde* had

demonstrated that he was not an "accidental browser" or "someone who took advantage of the free tour" offered by the site, but who, after viewing the contents, "balked at taking the active steps necessary to become a member." *Gourde,* at 1070. By contrast here, the NIT warrant did nothing to distinguish between "accidental browsers" (or even people looking for legal pornography or more extreme, but still legal, fetish content) and people who, like the defendant in *Gourde*, had viewed samples of the child pornography on offer and then chose not only to join the site, but pay for a continuing membership. Here, a person who landed on Playpen and entered an email and a username, were without anything additional, automatically subjected to a search and monitoring by deployment of the NIT

Considering whether accidental browsers created probable cause for a search, the Second Circuit in *Falso*, held that the mere fact the defendant had apparently tried to access a non-membership website called www.CPfreedom.com featuring images of child pornography, absent any evidence that he subsequently viewed those images, did not establish probable cause to search his computer. *Id*. at 121. Distinguishing *Martin*, the Court emphasized Martin's registration in a members-only pornographic website to the finding of probable cause in that case because "membership in the e-group reasonably implied use of the website," *id*., quoting *Martin*, 426 F.3d at 75. The Court stressed that "it [wa]s the fact of membership to a child-pornography website that largely supports the inference[ ] . . . that the defendant more likely than not used the website and downloaded images from it." *Id*. Absent similar circumstances suggesting that *Falso* had come upon the website for the purpose of finding child pornography, the Court held that the mere fact that he visited or tried to visit a website that could have provided access to pornographic images did not create a fair probability that he subsequently obtained access to those images. *Id*. at 120. Here, the obviousness of the content of the site was lacking unlike

Martin.

If the Second Circuit declined to find probable cause based on *Falso's* mere access of a website called CPfreedom, then this Court should undoubtedly hold that Mr. Stacey's visit to a site called Playpen would equally lack a basis for probable cause to issue a warrant to search his computer. Unlike *Martin*, the NIT warrant in this case was issued upon a simple login to the site rather than a continuing membership after the visitor had a chance to see the contents of the site. Nothing was specific to the acts of Stacey other than the login. The login page of the website—even if it actually featured what the affidavit said it did—would still not "unabashedly announce" to a visitor that it was a child pornography website. However, even if it had been called "CP freedom",[6] the Second Circuit has made perfectly clear that merely logging into the site would not constitute probable cause.[7]

In this case, the affidavit attempted to mitigate this deficiency by claiming that "numerous affirmative steps" were required for users to locate Playpen on the Internet, and therefore it was "extremely unlikely that any user could simply stumble upon [it] without understanding its purpose and content." Ex. 1 at ¶ 10. This claim is patently untrue. For anyone who has even a passing familiarity with the Tor network, these statements are nonsense. In fact, the discovery in *United States v. Lorente;* CR15-274-MJP, shows that Playpen came to the attention of law enforcement in the first place because investigators were able to find it because the site was accessible on both the regular Internet and Tor network. Moreover, contrary to the affiant's claim

[6] "CP" is a widely used and known acronym for Child Pornography. See Wolak, J., et al. Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. *Child Abuse & Neglect* (2013), http://dx.doi.org/10.1016/j.chi.abu.2013.10.018

[7] The Second Circuit has expressed its concern over the ease at which an individual may inadvertently become a member of a child pornography e-group and basing probable cause on guilt by association rather than particularity and the protection of privacy. *United States v Coreas,* 419 F.3d 151, 158-159 (2d Cir. 2005)

that sites cannot be found on the Tor network with the equivalent of a "Google" search (Ex. 1 at ¶ 12), the Tor browser looks like a regular browser and there are a variety of Tor search engines.[8] A user need only enter search terms for sexually oriented sites, chat rooms, or a host of other content not related to child pornography to find sites like Playpen. *See, e,g.*, https://ahmia.fi/search (a search engine which interfaces with both the regular Internet and allows users to use search terms to find sites on the Tor network). The application also falsely claimed that "Tor hidden services are not indexed like web sites on the traditional Internet." Ex. 1 at ¶ 12. In fact, the Tor network offers numerous "indexes," which contain links to all sorts of sites with sexual content that may or may not be legal. *See, e.g*, http://thehiddenwiki.org/ (the most popular Tor index, which also lists, contrary to the affiant's claims, a variety of Tor search engines). Furthermore, the fact that some visitors were using a Tor server is not indicative of criminality. *See United States v. Galpin*, 720 F.3d 436, 446-447 (2d Cir. 2013) *accord United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1176 ("CDT") (9th Cir. 2010) ("Wrongdoers and their collaborators have obvious incentives to make data difficult to find, but parties involved in lawful activities may also encrypt or compress data for entirely legitimate reasons: protection of privacy, preservation of privileged communications, warding off industrial espionage or preventing general mischief such as identity theft.").

With these principles in mind, the NIT warrant application was deficient and failed to make out probable cause under this circuit or any other circuits' standard of probable cause. This is especially true given that the application cannot be taken at face value. When this Court considers what the website actually looked like, and the lack of information showing that the site

[8] See https://www.torproject.org/projects/torbrowser.html.en

advertised itself as a source of child pornography, there can be no reasonable dispute that the issuing magistrate would not have granted the warrant if she had been presented with the complete and accurate facts that were known to the FBI at the time.

B. The Court Should Hold a *Franks* Hearing Because the NIT Affidavit Contains, at a Minimum, Recklessly Misleading Statements and Omissions.

The facts alleged in the warrant application cannot be taken at face value, because several critical allegations were false or misleading. Most importantly, the application falsely described the Playpen homepage. The application also portrayed the Tor network as solely serving a nefarious purpose. The application also inaccurately portrayed and over broadly portrayed what Mr. Stacey may have seen after he entered a username and email.

In *Franks v. Delaware*, 438 U.S. 154, 156 (1978), the Supreme Court held that "where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." This doctrine also applies to omissions that are the result of the affiant's "reckless disregard for the truth" of information which is material to a finding of probable cause. *United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000). *Franks* also protects against technically true claims that are designed to mislead, or that are made in reckless disregard of whether they would mislead, the magistrate. *United States v. Awadallah*, 349 F.3d 42, 68 (2d Cir. 2003) quoting *United States v. Colkley*, 899 F.2d 297, 300-01 (4th Cir. 1990)

Evidence obtained pursuant to an affidavit containing erroneous or misleading information must be suppressed when the misleading inaccuracies or omissions were necessary to the issuing judge's probable cause finding. *United States v. Canfield*, 212 F.3d 713, 717-18

(2d Cir. 2000). In the case of omissions, "the ultimate inquiry is whether, after putting aside erroneous information and correcting material omissions, there remains a residue of independent and lawful information sufficient to support a finding of probable cause or necessity." *United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013) *quoting Canfield*, 212 F.3d at 718. The Second Circuit "gauge[s] the materiality of the misstatements by a process of subtraction." *Id.* at 65. To determine if the false information was necessary to the issuing judge's probable cause determination, i.e., material, "a court should disregard the allegedly false statements and determine whether the remaining portions of the affidavit would support probable cause to issue the warrant." *Id.* If the corrected affidavit still supports probable cause, the inaccuracies were not material to the probable cause determination and suppression is inappropriate. *Canfield*, 212 F.3d at 718 (quoting *United States v. Trzaska*, 111 F.3d 1019, 1027-28 (2d Cir. 1997)).

In this case, the false and omitted statements were clearly material. The false and inaccurate description of the Playpen homepage was a primary component of the affiant's allegation in support of probable cause. The FBI propagated this falsity to deceive the Magistrate Judge that the site was not only "dedicated" to child pornography, but that this purpose would be apparent to anyone who viewed its public homepage and therefore would know the criminal nature of what they were getting into. After all, the affiant's burden was not simply to show that that Playpen contained child pornography; they had to demonstrate probable cause that those who visited the website did so with the purpose of accessing child pornography. If the former was all that was required then someone could have their home searched simply for entering an

adult bookstore that sold child pornography under the counter, even though the visitor was only looking for a 'Playboy' magazine, or for that matter, the cheaper imitator, a 'Playpen' magazine.[9]

The affidavit misled the Magistrate that entrants to the Playpen site knew what they were getting into by including a patently inaccurate description of the website in the supporting affidavit, despite the fact that the FBI well knew before applying for the warrant that it was inaccurate. It is clear the FBI knew what was featured on the homepage because they were the ones running and administering the site at the time. These facts alone warrant a *Franks* hearing, but to make matters worse, the inaccurate description of the homepage was accompanied by other false statements and omissions that, taken as a whole, resulted in a highly misleading affidavit.

In addition, the description of the Tor Network was equally misleading. First, Tor can be searched and has a number of perfectly legitimate users and reasons for its existence outside the realm of child pornography. Instead, the statements in the NIT application make it appear that anyone who found Playpen must have been determinedly seeking child pornography are simply not true. To the contrary, once someone has downloaded the free Tor browser package that connects them to the network they can explore it with a Tor search engine similar to Google or Bing. *See, e.g*, https://ahmia.fi/search. Using search terms for legal content, such as "sex chat" or "teen erotica," can readily lead Tor browsers to a variety of sites like Playpen, which do not contain illegal images. *See generally United States v. Hill*, 459 F.3d 966, 970 (9th Cir. 2006) ("Child pornography is a particularly repulsive crime, but not all images of nude children are pornographic.... Moreover, the law recognizes that some images of nudity may merit First Amendment protection because they serve artistic or other purposes, and possessing those

[9] See again Playpen magazine, Ex. 7

images cannot be criminal"). These facts, coupled with the absence of any images of "prepubescent" girls or even clear indication that the site contains pornographic pictures (let alone child pornography), are inconsistent with the portrait the affiant was trying to paint of a site that "advertises" itself as "dedicated" to child pornography.

The Government also devoted a substantial portion of the application to describing commonplace features of the site, while at least suggesting that these features were indicative of criminality. For example, the affiant stated that the site "allows users of the TARGET WEBSITE to upload links to images of child pornography that are accessible to all registered users of the TARGET WEBSITE." Ex..1 ¶ 23. This statement, although technically true, is calculated to mislead. The same link and image upload capabilities described by the affiant are basic features of myriad web sites that enable users to post messages and pictures, including everything from pictures of baked goods (*see, e.g*, epicurious.com) to YouTube videos.

Likewise, the affidavit mislead the Virginia Court by stating that the ability of users to exchange names and messages on the site are features "commonly used by subjects engaged in the online sexual exploitation of children." Ex. 1 ¶ 25. These very same features are offered by Twitter and Facebook, among many others. Suggesting that they are in any way indicative of criminality is similar to asserting that bank robbers "commonly" use cars to make a getaway. Millions of innocent people have cars, and the mere fact that someone has a car does not remotely support the conclusion that he or she is likely to be a bank robber. Likewise, billions of e-mails and text messages are sent every day—some of them undoubtedly are used to facilitate any number of illicit activities—but allowing the FBI to suggest that anyone who texts or e-mails may be involved in a crime begs incredulity and sets a chilling precedent.

Excising these false and misleading claims and omissions leaves virtually nothing upon which to find probable cause to search. The corrected affidavit could allege nothing more than that Mr. Stacey merely visited a website that happened to contain some child pornography which was not visible when he entered the website. There would be nothing to even suggest that he was aware it contained child pornography or that he intended to access child pornography; this would simply not be enough without something more that indicates that he actually participated in the illegal activities of the group. This circuit has held that even where a person visits a website named CPfreedom.com, probable cause does not exist simply from a visit or association. See *Falso*, 544 F.3d 110, 120 (2d Cir. 2008) (Second Circuit holding that there was no probable cause where "affidavit alleged only that [defendant] was perhaps one of several hundred possible subscribers to the cpfreedom.com website, who appeared either to have gained or attempted to gain access to the site.") *See also, e.g., United States v. Brown*, 951 F.2d 999, 1003 (9th Cir. 1991) (ruling that individual officer's membership in corrupt police unit was not sufficient for probable cause without further proof that the officer actually participated in illegal activities); *United States v. Rubio*, 727 F.2d 786, 793-94 (9th Cir. 1984) (declaring that membership in Hell's Angels, standing alone, is not sufficient for probable cause without particularized allegation that the individual participated in the organization's criminal activity). All things considered, the affidavit, stripped of its false statements would not support probable cause, and a *Franks* hearing is required on this issue.

C. The NIT Warrant was Unconstitutionally Overbroad

The NIT warrant authorized the search of a computer. The FBI applied for the warrant because it knew installing malicious code on computers which removes data therefrom constitutes a search implicating the Fourth Amendment. The fact that this search was done using

advanced and still classified code does not change this analysis. The Circuit has held that "[l]ike 18th Century 'papers,' computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion. If anything, even greater protection is warranted." *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013).

The Fourth Amendment provides:

> " . . . no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The Second Circuit recognizes that the amendment has several component parts. First there is what Judge Pratt called the "probable cause prong." *United States v Young*, 745 F.2d 733, 758 (2d Cir. 1984). The probable cause prong was thoroughly discussed above, but the warrant in this case also fails on the "particularity prong."

The "particularity prong" defines the constitutional limits of an authorized search. It asks: where may the searchers go; and what may they seize? *Young*, 745 F.2d 733, 758 (2d Cir. 1984). Therefore, "[p]robable cause to search somewhere and seize something may exist; nonetheless, the warrant is invalid unless it contains language "particularly describing the place to be searched, and the…things to be seized. The need for such language is not merely a matter of form, to be disregarded in hard cases. It is the Constitution's command, to be obeyed in all cases." *United States v. Buck*, 1986 U.S. Dist. Lexis 16935, *3 (S.D.N.Y. Dec. 4, 1986).

In this case, the NIT warrant application sought an unprecedentedly sweeping exercise of search and seizure powers. Unlike a typical search warrant based upon facts establishing probable cause to search a particular location, the warrant gave the FBI broad discretion in deciding when and against whom to deploy the NIT. Specifically, the warrant authorized NIT

searches any time someone accessed Playpen's home page, regardless of whether they merely utilized its "chat" forum or their actual activities on the site. *See generally* Kevin Poulsen, *Visit the Wrong Website, and The FBI Could End Up in Your Computer*, Wired.com, August 5, 2014 (although targeted use of "malware" by the FBI is not new, "[w]hat's changed is the way the FBI uses its malware capability, deploying it as a dragnet instead of a fishing line")

As a result, the NIT warrant may fairly be characterized as the Internet age equivalent of a general warrant, allowing the FBI to search tens of thousands of computers for which probable cause to search was not established. The warrant could easily have been narrowed to authorize searches of only those site visitors who viewed or downloaded illegal pornography, an appropriately circumscribed line to draw given that illicit content was contained in specific sub-directories on the site. Since the FBI could send its malware to anyone who logged into the site, the warrant could simply have required the FBI to target only those people who "clicked" on particular sub-directories with illegal content or particular pictures or links in those sub-directories. Indeed, in a footnote, the affiant acknowledges that the FBI could do exactly that, yet the warrant does nothing to particularize or narrow the set of visitors who would be subjected to searches. Ex. 1 at ¶ 24, n. 8.(" . . . the FBI may deploy the NIT more discretely against particular users, such as those who have attained a higher status on Website 1 by engaging in substantial posting activity). The fact that the FBI was running the website would have made this incredibly easy.

"The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.'" *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (*quoting Payton v. New York*, 445 U.S. 573, 583 (1980)). "The clause was intended as a bulwark against the 'general

warrant' abhorred by the colonists and protects against a general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

The Second Circuit has undertaken the challenge of applying 18th century notions about searches and seizures to modern technology and measured Government actions taken in the "computer age" against Fourth Amendment frameworks crafted long before this technology existed. *United States v. Ganias*, 755 F.3d 125, 133 (2d Cir. 2014). The Second Circuit has concluded that "[i]f anything, *even greater protection is warranted*" for computer files than any mail or paper. *Id. See also, e.g., Galpin*, 720 F.3d at 446 ("[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain.").

The FBI has engaged in the very basic governmental wrong that the Fourth Amendment was enacted to protect against. The FBI sought the broadest possible search authorization, capturing untold thousands of targets in their dragnet, and made no effort to narrow or focus that authorization. In sum, the FBI filed a misleading affidavit that deceived a magistrate into issuing the digital age equivalent of a general warrant. With the *Franks* violations taken into consideration, the overbreadth of the warrant is even more striking and, standing alone, warrants suppression. *United States v. Hickey*, 16 F. Supp. 2d 223, 239 (E.D.N.Y. 1998) (warrant without "meaningful parameters to guide the executing officers" warrants suppression) citing *United States v. Kow*, 58 F.3d 423 (9th Cir. 1995) (rejecting good faith exception and affirming suppression order for search undertaken pursuant to an overbroad warrant). *See also United States v. Galpin*, 720 F.3d 436, 453 (2d Cir. 2013) (affirming the district court's determination that the warrant application failed to establish probable cause to search for evidence of child pornography were the warrant was impermissibly broad.)

D. The NIT Warrant was an Anticipatory Warrant and Irrespective of the Misleading Claims in the Supporting Affidavit, was Triggered Prematurely.

The Second Circuit has cautioned that "[a]ny warrant conditioned on what may occur in the future presents some potential for abuse." *United States v. Garcia*, 882 F.2d 699, 703-704 (2d Cir. 1989). Therefore, the Circuit has warned that "Magistrates and judges should take care to require independent evidence of criminal activity giving rise to probable cause before issuing such a warrant. *Id*. "This means that affidavits supporting the application for an anticipatory warrant must show, not only that the agent believes a delivery of contraband is going to occur, but also how he has obtained this belief, how reliable his sources are, and what part government agents will play in the delivery." *Id*. Thus, "when an anticipatory warrant is used, the magistrate should protect against its premature execution by listing in the warrant conditions governing the execution which are explicit, clear, and narrowly drawn so as to avoid misunderstanding or manipulation by government agents." *Id*.

Assuming, for the sake of argument, that the warrant application's description of "pornographic" pictures on the home page had established probable cause to believe that anyone who entered the site was a legitimate search target, the foundation for that conclusion was undermined when that description proved to be inaccurate. Without illegal images on the public home page, all that remains to establish probable cause is the technical verbiage on the home page, which is not indicative of illegal activity; general and erroneous assertions about how sites can be found on the Tor network; and the allegations about the site's content. The content, moreover, is largely irrelevant because the warrant authorized searches before users could even see that content.

Given these facts (or lack of them), there can be no reasonable dispute that the home page, as it actually appeared when the warrant was approved and when the searches were

executed, contains little, if anything, that would lead an unwitting visitor to believe that Playpen was more than a common pornography site or sexually oriented chat room. As a result, the triggering event as established in the warrant application, the visiting of an obviously illegal website, could not, and did not, occur. Since the triggering event could not occur, any searches based on the NIT warrant inevitably exceeded the scope of its authorization.

Nevertheless, without alerting the issuing Virginia Magistrate to its errors or submitting a revised warrant application, the Government proceeded to alter and search the computers of site visitors for at least two more weeks as if nothing had changed. The content of the site on the date of the initial registration was a key fact, specific to each visitor, and relied on to issue the warrant. Absent an accurate accounting of the content and its apparent advertisement of child pornography when those searches were executed, the trigger for probable cause was lacking. Consequently, when the Government proceeded with the NIT searches anyway, it was acting outside the scope of the warrant, and suppression is required. *See e.g. Garcia, 882 F.2d 699, 703-704* (2d Cir. N.Y. 1989)(*citing Stanford v. Texas*, 379 U.S. 476, 485 (1965) (search warrant must contain descriptions reflecting "the most scrupulous exactitude"). Here, the triggering event came prematurely—before there was probable cause that any crime had been committed—therefore, this is the type of invalid anticipatory warrant the Second Circuit has cautioned against. Accordingly, the fruits of this unconstitutionally impermissible warrant must be suppressed.

E. The NIT Search and Seizure of Information from Mr. Stacey's Earlton, New York Computer was not Authorized by the Warrant Which Only Authorized a Search on Property *Located in the Eastern District of Virginia*

Based on the express language of the NIT warrant itself, the Court can and should grant an order of suppression for the simple reason that the FBI searched the wrong location.

To begin, the cover sheet of the NIT application (the first thing the issuing judge would have looked at to determine the location of the proposed search) reads as follows:

> I, a federal law enforcement officer or an attorney for the Government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property. . . *located in the Eastern District of Virginia*, there is now concealed (see attachment B).

Consistent with this sworn statement, the NIT warrant itself only authorizes searches of "person or property located in the Eastern District of Virginia." Ex. 1.

To state the obvious, when a warrant authorizes searches in one location, it does not authorize searches in other locations. *Walter v. United States*, 447 U.S. 649, 656 (1980) ("When an official search is properly authorized – whether by consent or by the issuance of a valid warrant – the scope of the search is limited by the terms of its authorization."); *see also, e.g., Simmons v. City of Paris, Tex.*, 378 F.3d 476 (5th Cir. 2004) (warrant for 400 N.W. 14th Street did not justify search of 410 N.W. 14th Street)); *Pray v. City of Sandusky*, 49 F.3d 1154 (6th Cir. 1995) (warrant for 716 ½ Erie Street, upper level of a duplex home, did not justify search of 716 Erie Street, lower level of the duplex; affirming denial of qualified immunity for officers involved in search). Therefore, there is no constitutionally permissible way a warrant to search a computer located in Virginia, could be used to search a computer in New York.

Here, the FBI plainly violated the express terms of the NIT warrant by searching a location in New York State (Mr. Stacey's home computer). In response, the Government will no doubt note that the warrant's "Attachment A" ("Place to be Searched") refers to the "activating computers" of "any user or administrator who logs into" Playpen. However, this attachment is incorporated by the warrant solely to identify "the property to be seized" that is "now concealed" in the Eastern District of Virginia, and does not alter the specific location stated on the face of the warrant itself.

Consistent with this conclusion, the attachment itself does not reference any locations other than the EDVA or otherwise expand the geographic boundary imposed by Magistrate Judge Buchanan on the face of the warrant. Accordingly, while a fair reading of the warrant and attachment does authorize searches of "activating computers" wherever they may be located in the Eastern District of Virginia, there is nothing within the four corners of the warrant that alters its plain language or can reasonably be construed to expand the search authorization to anywhere in the world. Suppression is required for all data that was seized outside of the warrant's express and limited authorization. *Marron v. United States*, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible ***and prevents the seizure of one thing under a warrant describing another***.")(emphasis added). It is therefore axiomatic that a warrant describing and authorizing a search of property in Virginia could not be used to search property in New York.

F. The NIT Warrant Violated Rule 41 and Suppression is Required

The Government's search of the Mr. Stacey's computer was conducted in violation of the jurisdictional requirement for searches under Fed. R. Crim. P. 41 and 28 U.S.C. § 636(a). This requirement authorizes a magistrate judge to issue a search warrant only for a location within the issuing judicial district itself, with very limited exceptions not applicable in the present case. This restriction is not a technicality. Rather, Rule 41 and § 636(a) serve as a fundamental safeguards against nationwide dragnet searches. The Second Circuit has held that violations of Rule 41 should lead to exclusion where (1) there was "prejudice" in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule. *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975).

i. The Warrant Violated Rule 41

Rule 41 limits the authority of a magistrate judge to issue warrants to search for and seize a person or property located within their district. The searches of the defendant's home and computer devices on January 28, 2016 were the direct result of the illegal search of his computer—and countless others[10]—through the use of a NIT. The NIT Warrant issued by a magistrate judge of the Eastern District of Virginia violated the clearly established jurisdictional limits set forth in Fed. R. Crim. P. 41. It allowed government agents to conduct a borderless dragnet search with no geographic limitation. Rule 41 simply does not permit a magistrate judge in Virginia to authorize the search of the defendant's computer located in New York.

Rule 41(b) provides a magistrate judge with authority to issue a warrant in five unambiguous circumstances, included in relevant part below:

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
>
> > (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a **person or property located within the district**;
> > (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is **located within the district** when the warrant is issued but might move or be moved outside the district before the warrant is executed; . . .[11]

The warrant in this case was not authorized under any of these sections and is therefore plainly unlawful. The Supreme Court has held that "property" as described in Rule 41 includes intangible property such as computer data. *See United States v. New York Tel. Co.*, 443 U.S. 159,

[10] See Joseph Cox, The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers, January 5, 2015, available at: http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers

[11] Rule 41 has since been amended with the amendment effective on December 1, 2016. Such amendment only serves to strengthen Stacey's argument that the court acted without appropriate authority. *See* Fed. R. Crim. P. Rule 41(b), Advisory Committee Notes, Subdivision (b), *2016 Amendments* (Reiterating constitutional requirements still must be met but clarifying the "venue" components of the statute and adding two instances where a court will have the authority to issue a warrant for remotely accessing electronic media outside the court's jurisdiction).

170 (1977). The searches of computer data were confined to that which was residing in the Eastern District of Virginia according to the language of Rule 41 and the Supreme Court's interpretation of property. Although the Supreme Court has not addressed this specific issue, other district courts have supported this position by suggesting that Rule 41 restricts electronic searches to the district in which the warrant was issued. *United States v. Glover*, 736 F.3d 509, 514-515 (D.C. Cir. 2013). *See also In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 756 (S.D. Tex. 2013) (rejecting government's application for a warrant to deploy software to remotely extract identifying information from a computer in an unknown location, because "there is no showing that the installation of the 'tracking device' (i.e. the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet."). Thus, the search of Mackenzie Stacey's computer in New York could not be authorized by a search warrant issued in the Eastern District of Virginia and all information procured as a result should be suppressed. *See United States v. Croghan*,__F.Supp.3d___, 2016 WL 4992105, *2 (S.D. Iowa 2016)

ii. The Warrant is Not Authorized Under Rule 41(b)(1).

Rule 41(b)(1) allows a magistrate judge to issue a warrant for people or property located within that judge's district. The NIT Warrant inaccurately states that the evidence sought is "located in the Eastern District of Virginia." Attachment A to the NIT Warrant indicates that the computer server, located in Virginia, is the place to be searched. Ex. 1, Attachment A. Yet the server for the "Target Website" was already under FBI control in the district. The actual "place to be searched" was the myriad of "activating computers — wherever located" that would unknowingly download the NIT, thereby forcing the transmission of their internal data back to the FBI in Virginia. See Ex. 1 at ¶ 46. The NIT Warrant authorized these searches even though there was no basis from which to conclude that these computers would be located in the Eastern District of Virginia.

Rule 41(b)(1) cannot be the basis for the search of the defendant's computer in New York. Lest there be any doubt about whether it was the defendant's computer that was searched rather than the Virginia server, the Government explained the need for the NIT on the basis that possession of the server alone would not allow the Government to identify the site's users in order to monitor their communications. Ex.. 2 at ¶ 58. In order to do so, it was necessary to deploy the NIT so that the defendant's computer would download the NIT and allow the Government to seize this information in New York before sending it to Virginia. Thus, although the NIT was first deployed from the server in Virginia, it is clear that the actual search occurred when the NIT was installed on the defendant's computer and extracted its data. This situation is no different from agents claiming that a search took place in Virginia because they traveled to Earlton, New York, copied data from a computer, and returned to Virginia before examining the contents. The fact that the Government is now capable of seizing data on a computer without

physically traveling to its location does not alter this analysis. In another Playpen case, *United States v.Croghan,* the district court found in the face of an apparent government concession, that the warrant could not issue because the search would be occurring outside the Eastern District of Virginia. 2016 WL 4992105, *3. As is the case here, the search was of the defendant's computer, which was never located in the Eastern District of Virginia. *Id.*

The Court reached a similar conclusion in denying an application to issue a search warrant in *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) ("*In re Warrant*"). There, the location of the target computer was unknown but the Government relied on Rule 41(b)(1) by reasoning that the "information obtained from the Target Computer will first be examined in this judicial district." *Id*. at 756. In rejecting the application, the court explained that the search and seizure of data occurs "**not in the airy nothing of cyberspace, but in physical space with a local habitation and a name.**" *Id*. The same is true here: the NIT search of Mackenzie Stacey's computer did not take place in "the airy nothing of cyberspace," and it did not take place in the Eastern District of Virginia. The search took place in Earlton, New York, which is beyond the jurisdiction of the court in Virginia.

iii. The Warrant is Not Authorized Under Any of the Other Subsections of Rule 41(b).

The other subsections of Rule 41(b) are inapplicable to this case. Rule 41(b)(2)—which allows an extraterritorial search or seizure of moveable property if it is located within the district when the warrant is issued, but might move or be moved before the warrant is executed—fails to provide authorization because the defendant's computer was never physically within the Eastern District of Virginia. *See Croghan,* 2016 WL 4992105 *4-5 (rejecting the argument that the crimes were committed when the out of state computer logged into the location of Website A, Eastern District of Virginia, because the users were travelling into the Eastern District via their

computers). *See also United States v. Levin*, 2016 WL 2596010, at *12 (D. Mass. May 5, 2016) (finding the NIT Warrant substantively violated Rule 41(b) and was void ab initio).

Importantly, the court in *In re Warrant* noted:

> That (b)(2) does not authorize a warrant in the converse situation—that is, for property outside the district when the warrant is issued, but brought back inside the district before the warrant is executed. A moment's reflection reveals why this is so. If such warrants were allowed, there would effectively be no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found. 958 F. Supp. 2d at 757.

Rule 41(b)(4) allows for tracking devices to be installed within the issuing district on an object that may travel to outside the district. The NIT here was installed on the defendant's computer in Earlton, New York which was never physically located within the Eastern District of Virginia. See *Michaud*, 2016 WL 337263 at *6. Even if the installation were deemed to have occurred on the server in Virginia, section (b)(4) is inapplicable because the defendant "never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district." *See id*. Sending the NIT code was not a "tracking device" but rather a way that information was extracted from the host computer, making 41(b)(4) inapplicable. *Croghan*, 2016 WL 4992105 *4-5.

iv. The Warrant Also Violated 28 U.S.C. § 636(a).

The search warrant issued by the magistrate judge in the Eastern District of Virginia also was in violation of the Federal Magistrates Act. *See Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring) (emphasizing that a violation of Rule 41(b)'s territorial limitations also implicates a statutory limitation). Section 636(a) provides three geographic areas in which a magistrate

judge's powers are effective, none of which applies here. See *id*.[12] Thus, the NIT Warrant not only violated Rule 41, but also Section 636(a) of the Federal Magistrates Act.

Suppression is required because the Rule 41 violation also implicates Section 636(a). See 28 U.S.C. 636(a). The issuing magistrate judge lacked statutory authority to issue the NIT warrant in the first place. *See Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring). Importantly, "Section 636(a)'s territorial restrictions are jurisdictional limitations on the power of magistrate judges and the Supreme Court has long taught that the violation of a statutory jurisdictional limitation— quite unlike the violation of a more prosaic rule or statute—is per se harmful." *Id*. at 1122 (emphasis in original).

v. The Violation of Rule 41 Requires Suppression because it was Prejudicial and of a Constitutional Magnitude

The magistrate judge was never authorized to issue the NIT warrant and therefore its use constitutes Government hacking of the defendant's computer rather than a lawful search. "[A] warrant issued in defiance of positive law's jurisdictional limitations on a magistrate judge's powers . . . for Fourth Amendment purposes. . . . is no warrant at all." *See Krueger*, 809 F.3d at 1126 (Gorsuch, J., concurring). This violation of a jurisdictional statute mandates suppression to preserve judicial integrity and proper separation of powers under the United States Constitution. *See id*. at 1123 (noting that § 636 is entitled "Jurisdiction, powers, and temporary assignment"). Moreover, violations of Rule 41 require suppression when a defendant is prejudiced by the lack of compliance. See *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975). "Prejudice means being 'subjected to a search that might not have occurred or would not have been so

[12] "Each United States Magistrate judge … shall have [1] within the district in which sessions are held by the [district] court that appointed the magistrate judge, [2] at other places where that [district] court may function, and [3] elsewhere as authorized by law … all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure. . . ." Id.

abrasive' had the rules been followed." *Id.* In the instant case, Mackenzie Stacey was prejudiced because the search authorized by the Residential Warrant would never have occurred but for information derived from the improperly issued NIT Warrant. It is the epitome of prejudice. Investigators discovered the defendant's alleged IP address through the use of the NIT. Ex. 1, ¶ 27. They then used this information to obtain the subscriber information for the IP address from Mid- Hudson Cablevision, which ultimately led them to obtain the Residential Warrant. Id. at ¶ 29.

The sole reason that investigators were able to identify Stacey and a residence where he lived was because they had already used the NIT Warrant to search his computer and obtain his IP address. Thus, if not for the NIT Warrant, there would have been no probable cause to support the Residential Warrant. Ex.. 2 at ¶ 58 ("deployment of a NIT to attempt to identify actual IP addresses used by TARGET SUBJECTS . . . is the only available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the identity of the TARGET SUBJECTS.") (emphasis added). The search of the defendant's property conducted on October 30, 2015, and his eventual statements to the agents would therefore never have occurred.

The unrestrained expansion of judicial authority to issue search warrants without geographic limitation is not a mere technicality. This violation of Rule 41(b) is not the type of "ministerial" violation for which courts have declined to require suppression. *See e.g., United States v. Dauphinee*, 538 F.2d 1, 3 (1st Cir. 1976) (steps required by Rule 41(d) are basically ministerial). This provision of rule 41, the authority of the magistrate judge to issue the warrant, involves the validity of the warrant. It is not a question of a ministerial act. *See Croghan* 2016 WL 4992105 (suppression required because a violation of Rule 41(b) is a jurisdictional flaw

which cannot be excused as a technical defect) (citing *Levin*, 2016 WL 2596010 and *United States v. Arterbury*, No. 15-cr-182, ECF No. 47 (N.D. Okla. Apr. 25, 2016) (quotations omitted).

The Court exceeded its authority by issuing a warrant for property located outside of its jurisdiction. The Court of Appeals for the District of Columbia considered a similar issue in *United States v. Glover*, 736 F.3d 509, 510-516 (D.C. Cir. 2014) where it suppressed the fruits of a Title III wiretap because the court had authorized the installation of a listening device outside of the District. The Court held that Rule 41(b), which partially implements Title III, is "crystal clear" and that "a jurisdictional flaw in the warrant" cannot be excused as a "technical defect." *Id*. at 515. The same logic applies with even greater force here. The agents in *Glover* could have simply obtained the warrant from a magistrate judge in Maryland or Virginia whereas in this case there is no magistrate judge with authority to issue the nationwide warrant.

Moreover, the court in *Glover* found a "blatant disregard of a district judge's jurisdictional limitation" where the warrant expressly authorized agents to enter the vehicle regardless of whether it was located in D.C., Maryland, or Virginia. 736 F.3d at 510, 515. In the instant case, the Government failed to comply with the Fourth Amendment's particularity requirements. U.S. Const. Amend. IV ("no warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched. . ."). The "manifest purpose of the particularity requirement of the Fourth Amendment is to prevent wide-ranging general searches by the police." *Bonner*, 808 F.2d at 866. Had the government particularly described the place to be searched, i.e., a computer in a residence in, Earlton, New York, a warrant could have issued. Instead, the search warrant erroneously described the place to be searched **as the server**, **located in Virginia**. See Ex. 1 Attachment A (emphasis added). "The test for determining the adequacy of the description of the location to be searched is whether . . . 'there is any reasonable

probability that another premise might be mistakenly searched.'" *Bonner*, 808 F.2d at 866. Because the magistrate in Virginia could not authorize a search of a computer in New York, its occurrence demonstrates that the description of the location to be searched was insufficient to prevent a reasonable probability of mistake. The fact that countless other computers were also searched only bolsters this conclusion.

Similarly, it described the information to be seized as data from the activating computers while overlooking the fact that such information could only be obtained by first searching and seizing the data from those computers. See Ex. 1 Attachment B, p. 102. When it comes to a constitutional concern such as the particularity requirement, the Government cannot be rewarded for vagueness. To do so would invite further violations and undermine the core requirement set forth in the Fourth Amendment. *See In re Warrant*, 958 F. Supp. 2d at 758 ("This particularity requirement arose out of the Founders' experience with abusive general warrants").

Finally, the agents acted in intentional and deliberate disregard of Rule 41. Even where no prejudice occurs, suppression is appropriate where the government was not acting in good faith. *See United States v. Leon*, 468 U.S. 897, 922 (1984); *Krawiec*, 627 F.2d at 582; *Dauphinee*, 538 F.2d at 3. Particularly where the Government moved Website A's server from North Carolina to Virginia, there can be no credible argument that officers reasonably believed that none of the 214,898 members of Website A were located outside of Virginia. See Ex. 1 Attachment A, ("The activating computers are those of any user or administrator who logs into the TARGET WEBSITE.") (emphasis added) ; Ex. 2 at ¶ 71, p. 156 ("*It is not presently known with any certainty where any of the remaining TARGET SUBJECTS reside.*"). It is evident from the plain language of Rule 41(b) that no interpretation would allow the search of potentially thousands of computers located outside the authorizing district.

In *In re Warrant*, the court stated that where the location of the Target Computer is unknown, "the Government's application cannot satisfy the territorial limits of Rule 41(b)(1)." 958 F. Supp. 2d at 757. It is unlikely that the Government was unaware of this opinion when it filed its application. In any event, the Government was clearly aware that the NIT Warrant was not authorized when it made its application in February, 2015. A memorandum addressed to the Committee on Rule of Practice and Procedure dated May 5, 2014, introduced a proposed amendment to Rule 41(b) that would authorize the use of the NIT Warrant. See Reena Raggi, Report of the Advisory Committee on Criminal Rules, May 5, 2014, at 319.[13] Specifically, proposed Rule 41(b)(6) "would authorize a court to issue a warrant to use remote access to search electronic storage media and seize electronically stored information inside or outside of the district: (1) when a suspect has used technology to conceal the location of the media to be searched." Rebecca A. Womeldorft, Transmittal of Proposed Amendments to the Federal Rules, Oct. 9, 2015, at 8.[14] Where the memorandum introducing the proposal states that the change "had its origins in a letter from Acting Assistant Attorney General Mythili Raman," it is not feasible that the Government was unaware that such searches were not authorized under Rule 41(b). See Report of the Advisory Committee on Criminal Rules, at 324-325((explaining that "a warrant for a remote access search when a computer's location is not known would enable investigators to send an email, remotely install software on the device receiving the email, and determine the true IP address or identifying information for that device.").

The fact that the proposal required an entirely new subsection to Rule 41(b)—rather than a clarification to an existing subsection—demonstrates that there is no reasonable interpretation of any provision in Rule 41(b) that would permit such a search. Rule 41(b) provides explicit

[13] Available at: www.uscourts.gov/file/15532/download
[14] Available at: http://www.uscourts.gov/file/18641/download.

geographic limits on the magistrate judge's authority to issue search warrants and, under the circumstances presented here, precluded her from issuing a warrant authorizing the search of property outside the district. The rule is clear. Any changes are for the United States Congress to address any shortcomings in the Rule. Such sweeping increases in judicial authority must come from Congress, not from courts. Until that occurs, searches like the one in this case violate Rule 41(b) and must result in suppression.

"Operation Pacifier" is unprecedented and has resulted in extensive litigation in other districts. This case is one of a handful in this district and within the Second Circuit. A non-exhaustive review of the cases decided so far may prove helpful to this court.[15] Several recent decisions arising from the same facts and circumstances before this Court may be instructive. These include: *United States v. Michaud*, 2016 WL 337263 (W.D.Wash. Jan. 28, 2016); *U.S. v. Stamper*, Case No. 1:15cr109 (S.D.Ohio Feb. 19, 2016); *United States v. Arterbury*, Case No. 1:15cr182 (N.D. Oklahoma); *United States, v. Levin*, 2016 WL 1589824 (D.Mass. April 20, 2016); *United States v. Croghan*, 2016 WL 4992105, *2 (S.D. Iowa, September 19, 2016) and *United States v Kim*, 2017 WL 394498 (E.D.N.Y. 2017).

All of these cases involve the same operation that led to the present charges against Mr. Stacey. All of the cases involve the NIT warrant that was issued by Magistrate Judge Buchanan in the Eastern District of Virginia. All of these five cases found that the NIT warrant violated Fed. R. Crim. P. 41(b). However, in *Michaud* and *Stamper*, the courts held that the violation of Rule 41 was a mere "technical violation" that did not prejudice the defendant. *Stamper* adopted the reasoning of *Michaud* that one has no reasonable expectation of privacy in one's IP address

[15] See Exhibit G for a more complete overview of decided and pending "Operation Pacifier" cases.

and such information, even when extraordinary means have been taken to secrete that information. The *Michaud* and *Stamper* approaches are not tenable under Second Circuit precedent.

In *Galpin*, the Second Circuit stressed the importance of privacy on computers and held that "even greater protection is warranted" for digital information. *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013). Finally, any suggestion that an expectation of privacy is not reasonable when using a Tor server begs incredulity because Tor was invented by, and is still used by the government, to protect their own privacy online. Therefore, the FBI's conduct in this case implicates fundamental privacy issues and exceeds the contours of appropriate law-enforcement investigation techniques.

The courts in *Levin* and *Croghan* concluded that the NIT Warrant purportedly sought to authorize a search of property located outside the district where the issuing magistrate judge sat. The magistrate judge had no jurisdiction to issue such a warrant under the first paragraph of Section 636(a). *Levin*, 2016 WL 1589824 and *Croghan*, 2016 WL 4992105, *2. Because the magistrate lacked authority to issue a warrant for a search of property outside of its jurisdiction, the warrant was void at the outset. *Levin at *12; Croghan at *6.* Ultimately, both courts suppressed all of the evidence which stemmed from the NIT warrant because the warrants were issued without judicial approval. The good faith exception did not apply for the same reason.

G. The Earlton Warrant is Based Upon Information Which Was Obtained as a Result of an Illegal Search and Seizure the Excising of Which Leads to a Lack of Probable Cause Requiring Suppression of the Results of the Illegal Entry and Search

Rule 41(b) violations require suppression of not only the NIT warrant, but all other evidence "obtained as a product of illegal searches and seizures." *United States v. Crawford*, 372 F.3d 1048, 1054 (9th Cir. 2004) (en banc) (citing *Wong Sun v. United States*, 371 U.S. 471, 484-88 (1963)). The information which was obtained from the NIT warrant was then used as the basis for the Earlton warrant leading to the search of Stacey's residence. The Earlon warrant is equally deficient because the information contained within the application were the fruits of an illegal search and seizure. Absent the tainted information: the IP address, the types of computers, the software used, the government would not have been able to locate the internet service provider, seek account information and owner identity from the internet service provider and obtain a physical location. "When an application for a search warrant includes both tainted and untainted evidence, the warrant may be upheld if the untainted evidence, standing alone, establishes probable cause." *Laaman v. Williams*, 973 F.2d 107, 115 (2d Cir.1992), *cert. denied*, 507 U.S. 954 (1993). Where improper material is included in a warrant application, the court should disregard that information and "determine whether the remaining portions of the affidavit would support probable cause to issue the warrant." *United States v. Canfield*, 212 F.3d 713, 718 (2d Cir. 2000). Absent the tainted information, the court has nothing upon which to issue a warrant for the Earlton address. *Id.* ("The ultimate inquiry is whether, after putting aside erroneous information and material omissions, 'there remains a residue of independent and lawful information sufficient to support probable cause.' ")(quoting *United States v. Ferguson*, 758 F.2d 843, 849 (2d Cir.1985)). The government would not have had the address.

As explained in detail above, the Earlton search warrant—and the subsequent seizure and search of Mr. Stacey's computer—as well as the statement of Mr. Stacey made to the FBI in October of 2015 are the "fruit" of the illegal NIT warrant. Because the NIT warrant is invalid, all these fruits of that initial illegal search must be suppressed.

H. The Statements Attributed to Mackenzie Stacey on October 30, 2015 are subject to suppression in violation of Miranda and the Fifth Amendment. Any information derived therefrom is suppressible as "fruits of the poisonous tree."

Mackenzie Stacey was questioned while in a custodial situation during which he was not free to leave. Having finished questioning his father and his wife, then his father individually, the authorities then questioned Mackenzie. While SA Paris and Fallon had given Mackenzie's father his *Miranda* rights upon questioning him, they failed to inform Mackenzie of his rights, ascertain whether he understood those rights and ask whether he wished to waive those rights. Ex. 6. Instead, SA Paris and Fallon immediately began questioning Mackenzie about his use, access, and ownership of the computers within the house. Mackenzie identified "his computers." Ex. 6. Mackenzie also admitted to using the Tor network. Id. At one point during the questioning Paris consulted with another officer who informed him that a computer Mackenzie identified as his was connected with Website A. Id. Returning to the questioning, Paris and Fallon finally advised Mackenzie of his *Miranda* rights which he immediately waived. Ex. 7.

The voluntariness of a confession is governed by the Fifth Amendment, under which no person "shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. "[T]he constitutional inquiry is ... whether the confession was free and voluntary; that is, [it] must not be exacted by any sort of threats or violence, nor obtained by any direct or implied promises, however slight, nor by the exertion of any improper influence." *Malloy v. Hogan*, 378 U.S. 1, 7, 84 S.Ct. 1489, 12 L.Ed.2d 653 (1964) (internal quotation marks omitted)

(citing *Bram v. United States*, 168 U.S. 532, 542–43, 18 S.Ct. 183, 42 L.Ed. 568 (1897)). An accused's confession cannot be admitted if it was obtained by "techniques and methods offensive to due process, or under circumstances in which the suspect clearly had no opportunity to exercise a free and unconstrained will." *Oregon v. Elstad*, 470 U.S. 298, 304, 105 S.Ct. 1285, 84 L.Ed.2d 222 (1985) (internal quotation marks and citation omitted).

Whether a confession is voluntary is determined based upon the totality of the circumstances centered around: (1) the characterstics of the accused; (2) the conditions of the interrogation, and (3) the conduct of law enforcement officials. Here the officers questioned Mackenzie in a houseful of law enforcement, while his family was also being held, during the early morning search of their home without informing of his Miranda warnings over a prolonged period of time. Ex. 6. [16]

In addition to the coercive nature of the questioning, the initial statement was obtained in violation of *Miranda*. 384 U.S. 436, 476 (1966). The subsequent attempt to mirandize Mackenzie was ineffective. S*ee United States v. Anderson*, 929 F.2d 96, 102 (2d Cir. 1991) ("[T]he use of coercive and improper tactics in obtaining an initial confession may warrant a presumption of compulsion as to a second one, even if the latter was obtained after properly administered *Miranda* warnings."). When the government employs a two-step interrogation depriving the defendant of his *Miranda* rights depends in part upon objective and subjective evidence surrounding the interrogations, guided by—but not limited to—the factors identified by the plurality in *Seibert*." *Moore*, 670 F.3d at 230 (internal quotation marks and citation omitted); *see also United States v. Capers*, 627 F.3d 470, 483–84 (2d Cir. 2010). The *Seibert* factors consist of:

[16] Absent from the police reports provided is the fact that his father suffered a medical emergency resulting in his transport to a hospital for treatment.

> (1) the completeness and detail of the questions and answers in the first round of interrogation, (2) the overlapping content of the two statements, (3) the timing and setting of the first and second interrogation, (4) the continuity of police personnel, and (5) the degree to which the interrogator's questions treated the second round as continuous with the first.

Capers, 627 F.3d at 475 (citing *Missouri v. Seibert*, 542 U.S. 600, 615 (2004). Here Mackenzie was completely unfamiliar with the criminal process. He had been subject to the acts of law enforcement in his house for over one hour. *Compare* Ex. 5 with Ex. 7. His family was also being held. After he gave his first statement and the search of the computer revealed the connection to Website A, he was advised of his rights and he waived them two minutes later. and continued to answer the officers questions. Ex. 7. Just as in *Seibert* and *Capers* the information used in the second round of questioning was essentially the same or based on information obtained from the first round. *Seibert* at 537; *Capers* at 474. As a result, both statements made by Mackenzie are subject to suppression unless the government can prove otherwise. *Seibert* at 622; *Capers* at 474, 485.

IV. CONCLUSION

For the reasons stated above, the faulty NIT search warrant, the violations of Rule 41, and the failure to advise of Miranda rights the tangible evidence and statements of Mackenzie Stacey should be suppressed. The Earlton warrant, the items seized from that search—including computers and other property taken from Mr. Stacey on October 30, 2015—and Mr. Stacey's October 2015 statements to the FBI are also fruits of either invalid NIT search warrant, or the failure to properly advise of Miranda right providing an additional basis for suppression.

DATED: February 17, 2017

Respectfully submitted,
LISA A. PEEBLES
Federal Public Defender

By: *PAUL EVANGELISTA*
Assistant Federal Public Defender
Bar Roll No. 507507
MOLLY CORBETT
Assistant Federal Public Defender
Bar Roll No. 105740
Office of the Federal Public Defender
39 North Pearl Street, 5th Floor
Albany, NY 12207